様式 C-19

科学研究費補助金研究成果報告書

平成　２１年　５月　１８日現在

研究種目：基盤研究(B)
研究期間：2006-2008
課題番号：18300031
研究課題名（和文）　リスク管理型個人情報保護共有フレームワーク

研究課題名（英文）　Risk-Managed Personal Information Sharing Framework

研究代表者　岩井原 瑞穂　(IWAIHARA MIZUHO)
京都大学・情報学研究科・准教授
40253538

研究成果の概要：
本研究では，利用者が自分の個人情報をサービスプロバイダに提供する際に，利用者が自らの判断に基づいて開示方式の選択を行なえるようにするため，利用者の判断材料となる情報開示リスクを提示し，またリスクを低減する開示方式を生成する枠組みの研究開発を行なう．具体的には，(1) 個人情報開示のためのリスク評価モデル，(2)リスクを考慮した個人情報保護共有方式，(3)個人情報保護共有のためのＸＭＬアクセス制御，(4)リスク管理型個人情報保護共有フレームワークの応用の４つのテーマに分けて研究を行なった．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	5,800,000	1,740,000	7,540,000
2007 年度	5,100,000	1,530,000	6,630,000
2008 年度	4,300,000	1,290,000	5,590,000
年度			
年度			
総　計	15,200,000	4,560,000	19,760,000

研究分野：総合領域
科研費の分科・細目：情報学・メディア情報学・データベース
キーワード：データベース，セキュリティ，プライバシー，XML，Web サービス

１．研究開始当初の背景

ネットワークを介して利用者が様々なサービスを利用するために，多様な Web サービスの連携が進められている．このようなサービスを利用するために利用者はアカウントを作成するとともに，住所氏名などの個人情報をサービスプロバイダに提供する必要がある．また利用者の購買履歴などの利用記録はサービスプロバイダにとっては経営戦略や効率化のための貴重な情報源である．しかしこのような利用記録もプライバシー情報に該当し，慎重な扱いを求められる．現在，日本や EU では個人情報保護法が制定され，個人情報の取り扱いの要件として，本人同意，利用目的の明示と遵守，管理の完全性・安全性，第三者授受制限，本人アクセスの提供等が個人情報取り扱い業者の義務として定められている．一方，サービスプロバイダからの個人情報の漏洩事件は多発しており，個人情報保護への対策が社会的要請となっている．利用者の利便性向上のためには，サービスプロバイダ同士が連携して個人情報や利用履歴を共有することは有効であるが，一方で共有により個人情報の目的外利用や漏洩のリスクは増大するともいえる．１つのサー

ビスプロバイダがアカウント管理や個人情報管理を集中して行なう方式が以前提唱されたが，個人情報を一箇所に集中させるリスクに利用者の抵抗感があり，支持が得られなかった．その後，サービスプロバイダ間でのアカウント管理の対等な連携（アイデンティティ連携）の標準的な枠組みとして Liberty Alliance が提唱され，多くの有力ベンダに支持されており，個人情報保護法への適合やシングルサインオンなどの技術仕様の策定が進められている．しかし個人情報を共有するサービスプロバイダ間の信用の輪（circle of trust）の形成や，利用者自身による個人情報開示の制御など，実現方法についてはまだこれからの段階である．

２．研究の目的

本研究では，利用者が自分の個人情報をサービスプロバイダに提供する際に，利用者が自らの判断に基づいて開示方式の選択を行なえるようにするため，利用者の判断材料となる情報開示リスクを提示し，またリスクを低減する開示方式を生成する枠組みの研究開発を行なう．具体的には，
(1) 個人情報開示のためのリスク評価モデル，(2)リスクを考慮した個人情報保護共有方式，(3)個人情報保護共有のためのＸＭＬアクセス制御，
(4)リスク管理型個人情報保護共有フレームワークの応用
の４つのテーマに分けて研究を行なう．

３．研究の方法

(1) 個人情報開示のためのリスク評価モデル
利用者が個人情報の入力をサービスプロバイダから求められた場合，求められている個人情報の属性がどのような性質であるかや，開示した場合のリスクについて知る必要がある．また姓名や住所，電話番号など単体で，あるいは組み合わせることによって，個人を特定される可能性のある属性がある（個人特定可能性）．また他人に知られたくないプライバシー属性として，趣味や宗教，学歴，職歴，病歴，年収など多くのものが挙げられる．提供する個人情報において，一般に個人特定可能性が低ければ，プライバシー性が損なわれる可能性は低くなる．サービスプロバイダが要求している属性が，利用者にとってどの程度のプライバシー性を持つかを利用者自身が判断できることが望ましいが，実際には属性が多岐にわたることや，サービス側の属性分類が一定しないことが予想されるため，利用者がプライバシーポリシーを設定する負担が大きい．そのため，本テーマではセマンティックWebの技術を用いて，プライバシー属性オントロジーを構築する．

(2)リスクを考慮した個人情報保護共有方式
リスクを低減する基本的な手法として，個人を特定する属性は非開示とし，代わりに（一時的な）アカウント(仮名)を用い，アイデンティティを隠蔽することが考えられる．また発展形として，電子商取引のワークフローの進行に応じ，実際にプライバシー情報が必要なステップに到達するまで開示を行なわないという，段階的な開示方式や，さらにアイデンティティプロバイダに公正な第三者の役割を行なわせる方式が考えられる．開示する情報のリスク評価に(1)のモデルを用い，さらに開示方式ごとのリスクを求める．さらに利用者自身が設定したリスク許容レベルの範囲内で開示を行なうことや，サービスプロバイダに対する信用度，共有するサービスプロバイダが多くなることによるリスクといった要素も考慮し，利用者の要求を満たす個人情報保護共有方式を自動的に選択する方式を開発する．
(3)個人情報保護共有のためのＸＭＬアクセス制御
インターネットでの情報交換にＸＭＬを用いるのが一般的となっており，ＸＭＬのアクセス制御は盛んに研究が行なわれている．本テーマでは，連携サービスプロバイダ間で効率よくアクセス制御の可否判定を行なう方式を開発する．これはアクセス制御ルールを表すプロバイダ間にまたがる大量の XPath 式を効率よく評価する方式である．
(4)リスク管理型個人情報保護共有フレームワークの応用
本研究課題の応用例として，いくつかの分野における個人情報保護共有のシステムを開発する．１つは電子商取引であり，利用者の設定したリスク許容度に基づく，段階的な属性開示方式の生成の実験を行う．

４．研究成果
(1) 個人情報開示のためのリスク評価モデル
個人情報漏えいのリスク評価手法として，本研究では日本ネットワークセキュリティ協会の提唱している経済的リスクと精神的被害リスクによるリスク評価手法を拡張した．オントロジー中の個体は，financialRisk(f-risk) と personalityRisk (prisk)の二種類のプロパティ値を持つ．これらはそれぞれ，属性をサービスプロバイダへ開示する際の金銭的なリスク値 rf (c), 精神的なリスク値 rp(c) を表しており，それぞれ [1.0,5.0] の実数値で示される．さらにこれらを重み付き加算した総合リスク値(combined risk value)を用いた．オントロジー中に要求されたプライバシー属性が存在しない場合，近接した概念のリスク値を用いる手法を

とった．そのため概念間の類似性を測る尺度としてJaro Winkler値とWordnet Similarityを重み付き加算したものを用いた．

一方，もうひとつのリスクモデルの研究として，大規模でかつ分散した組織においてロールベースアクセス制御を実装するシステムを導入する際に，セキュリティ上のリスクと，処理時間等のコストから，低減されるリスクを定量的に評価するモデルの開発も行った．セキュリティ上のリスクを分類し，想定した確率で生じるリスクから派生するイベントを故障木として表現する．そして特定のアクセス制御の実装方式を導入した際にどのくらいのリスク低減効果が得られるかを求めるた(I3E 国際会議でベストペーパ賞を受賞)．

(2)リスクを考慮した個人情報保護共有方式

サービスプロバイダの要求するプライバシー属性について，利用者が経済的および精神的被害リスク，総合リスクのいずれかの上限を許容値として与え，そのもとで開示可能な属性および値を選択する問題について取り組んだ．

サービスプロバイダが要求したプライバシー属性の集合とプライバシー属性オントロジーのクラス集合の間で属性の類似度を枝の重みとする重み付き二部グラフを構成し，許容リスク値の制約のもと，二部グラフの重みを最大化するようなマッチング問題を解く．これによりサービスプロバイダの要求する個人情報属性とプライバシー属性オントロジーのクラスを対応付けることが可能である．二部グラフの枝の重みとして，前述のオントロジーの概念とプライバシー属性間の概念的類似度を表す距離を用いる．３種類のリスク許容値の与え方により，いくつかの異なるマッチング問題を定式化できる．また，与えられたリスク許容値のもとで，概念的類似度を最大化する，あるいは与えられた概念類似度の範囲のもとで，リスクを最小化する，さらには概念的類似度とリスク値の双方を結合した目標関数を定義してその最大化を行う，といった目標の設定により異なるマッチング問題が定式化できる．大別して４つの問題を取り上げ，それぞれについて多項式時間で解くアルゴリズムを示した．

(3)個人情報保護共有のためのＸＭＬアクセス制御

XML 文書の量は急速に増え続けているが，特にニュース配信や wiki などでは，文書が随時更新されていく一方で，過去のデータへのアクセスも可能であることが多い．過去のデータに個人情報や企業の機密文書などの情報を含んでいる場合など，バージョンを持つ XML 文書のアクセス制御は，重要な課題の一つである．我々は XML 文書のバージョン管理とアクセス管理の統合概念を初めて指摘しており，バージョンの依存関係をもつ部分をまとめてアクセス制限を行うことを可能にするために，XML 文書の更新操作によって生じる依存関係に基づいたアクセス制御モデルの概念と，そのための XPath に時間軸の概念を導入した言語 XVerPath を提案している．本テーマでは，XML 文書の更新差分をデータベース管理する手法を開発し，その上で XVerPath の質問を評価する手法の開発を行った．XML 文書木に様々な工夫を施すことによって，XML 文書が更新されても新たな文書木を生成することなく，一つの木に変更の差分を保存し，任意の時刻のスナップショットを再現する手法や，文書のノード単位での派生関係を求める方法の開発を行った．

もうひとつの XML のアクセス制御手法として，ロールベースアクセス制御と細粒度の XML アクセス制御の統合した手法の開発を行った．アクセス制御の対象であるオブジェクトとユーザの対それぞれに対してアクセス制御ルールの設定および保存を行うことは空間コストや管理コストの面でも大きなコストになるため，ルールの対象を集約する必要がある．ロールベースアクセス制御について，XML 文書の木構造のみを利用し簡略化を行う既存手法に対して，XML 文書の木構造だけでなくロール階層の構造も利用し簡略化を行う手法を提案した．提案手法では，XML 文書内のある部分木の文書ノードとロール階層のあるロールから到達可能なロールの対の集合を DR 領域として定義し，集合の包含関係に基づき DR 束を構成した後，冗長なルールを削減する．またアクセス権限の変更，文書ノードの追加/削除，ロールの追加/削除といった更新操作について，更新の範囲を局所的に押さえた結果，更新コストを削減できることがわかった．

(4)リスク管理型個人情報保護共有フレームワークの応用

プライバシー属性オントロジーについて，既存のオントロジーツールを利用してオントロジーを構築するとともに，その上でサービスプロバイダが要求したプライバシー属性の集合とプライバシー属性オントロジーのマッチングを行う一連のアルゴリズムを実装した．またリスク値の設定を行ったり，アルゴリズムの選択や，マッチング結果の表示を行う利用者インタフェースの開発も行った．このインタフェースは，部分的な誤りを利用者が修正して，マッチングの再計算を行う機能も備える．利用者はこのインタフェースを通して，対話的に開示する属性および値を選択してゆくことができる．

評価実験として，代表的な電子商取引サイトを５つ，およびソーシャルネットワークサ

ービスを５つ選び，そこで要求されている属性集合を抽出してオントロジーに格納し，リスク値を与えた．これらのサイトのうちの１つをサービスプロバイダとして，残りの属性集合とマッチングする実験を行った．実験により，異なるマッチングのアルゴリズムの特徴を明らかにするとともに，得られた解の有用性を確認した．また，すべて十分実用的な時間で計算が行えることを確認した．

５．主な発表論文等
（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 10　件）

[1] Millist Vincent, Mukesh Mohania, and Mizuho Iwaihara, “Detecting Privacy Violations in Database Publishing using Disjoint Queries,”' Proc. 12th Int. Conf. Extending Database Technology (EDBT2009), pp. 252-262, Saint Petersburg, Mar. 2009 (査読有).

[2] Mizuho Iwaihara, Kohei Murakami, Gail-Joon Ahn, and Masatoshi Yoshikawa,"Risk Evaluation for Personal Identity Management Based on Privacy Attribute Ontology," 27th Int. Conf. Conceptual Modeling (ER2008), Lecture Note in Computer Science 5231, pp. 183-198, Barcelona, Oct 2008 (査読有).

[3] Seiichi Kondo, Mizuho Iwaihara, Masatoshi Yoshikawa, and Masashi Torato,
“Extending RBAC for Large Enterprises and its Quantitative Risk Evaluation," The 8th IFIP Conference on e-Business, e-Services, and e-Society (I3E 2008), Tokyo, pp. 99--112, Sep. 2008 (best paper award) (査読有).

[4] Yumi Yonei, Mizuho Iwaihara and Masatoshi Yoshikawa, “Person Retrieval on XML Documents by Coreference Analysis Utilizing Structural Features,” in Proc. 19h Int. Conf. Database and Expert Systems Applications (DEXA2008), Lecture Note in Computer Science 5181, pp.552-565, Turin, Sep. 2008(査読有).

[5] 米井由美, 岩井原瑞穂, 吉川正俊, “XML 文書における構造の素性を用いた照応による人物検索," 日本データベース学会論文誌, Vol.7, No.1, pp. 151-156, 2008 年 6 月(査読有).

[6] 村上耕平, 岩井原瑞穂, Gail-Joon Ahn, 吉川正俊, "アイデンティティ管理におけるプライバシー属性オントロジを用いた開示属性の分類,"日本データベース学会論文誌, Vol.7, No.1, pp. 55-60, 2008 年 6 月(査読有).

[7] 牛場祐貴, 岩井原瑞穂, 吉川正俊,``XML 文書のアクセス制御におけるロール階層を考慮したルール簡略化とルール変更操作の局所化," 日本データベース学会論文誌, Vol.7, No.1, pp. 49-54, 2008 年 6 月(査読有).

Century

[8] Mizuho Iwaihara, Somchai Chatvichienchai, Ryotaro Hayashi, Chutiporn Anutariya, Vilas Wuwongse, “Relevancy Based Access Control and Its Evaluation on Versioned XML Documents," ACM Transactions on Information and Systems Security, Vol. 10, No. 1, pp. 1-31, Feb. 2007(査読有).

[9] Sanjay Mittal, Rahul Gupta, Mukesh Mohania, Shyam Kumar Gupta, Mizuho Iwaihara, and Tharam Dillon, “Detecting Frauds in Online Advertising Systems," Proc. 7th Int. Conf on E-Commerce and Web Technologies (EC-Web2006), Lecture Note in Computer Science 4082, pp.222-231, Krakow, Sep. 2006 (best paper) (査読有).

[10] Somchai Chatvichienchai and Mizuho Iwaihara, “Detecting Information Leakage in Updating XML Documents of Fine-Grained Access Control,”' Proc. 17th Int. Conf. Database and Expert Systems Applications (DEXA2006), Lecture Note in Computer Science 4080, pp.286-296, Sep. 2006(査読有).

〔学会発表〕（計 8 件）

[1] 本村徹太郎，岩井原瑞穂，吉川正俊，”バージョン化されたXML文書に対する問い合わせの書き換え規則，” DEIMフォーラム 2009，掛川市, B7-2, 2009 年 3 月.

[2] 牛場祐貴，岩井原瑞穂，吉川正俊,“XML データベースのロール階層を考慮したアクセス制御におけるルールサマリを用いた高速化，” DEIMフォーラム 2009，掛川市，D4-1, 2009 年 3 月.

[3] 村上耕平, 岩井原瑞穂, Gail-Joon Ahn, 吉川正俊, “アイデンティティ管理におけるリスク評価に基づくプライバシー属性の開示判断支援,’’ Webとデータベースに関するフォーラム (WebDB Forum 2008),東京都, 2B-3, 2008 年 12 月.

[4] 米井 由美，岩井原 瑞穂，吉川 正俊，“XML文書における構造の素性を用いた照応による人物検索，” 電子情報通信学会第 19 回データ工学ワークショップ(DEWS2008)論文集， 宮崎市, C6-4, 2008 年 3 月.

[5] 村上 耕平, 岩井原 瑞穂, Gail-Joon Ahn, 吉川 正俊,”アイデンティティ管理における

プライバシー属性オントロジを用いた開示属性の分類," 電子情報通信学会第 19 回データ工学ワークショップ(DEWS2008)論文集, 宮崎市, C2-6,2008 年 3 月.
[6] 牛場 祐貴, 岩井原 瑞穂, 吉川 正俊, "XML文書のアクセス制御におけるロール階層を考慮したポリシー簡略化とポリシー変更操作の局所化," 電子情報通信学会第 19 回データ工学ワークショップ(DEWS2008)論文集, 宮崎市, C2-5, 2008 年 3 月.
[7] 近藤 誠一, 岩井原 瑞穂, 吉川 正俊, 小宮 崇, 山田耕一, 大沼 聡久, "ロールベースアクセス制御におけるロールの分散実装方式とそのＩＣカード運用管理への適用," 夏のデータベースワークショップ 2007 (DBWS2007), 仙台市, 2007 年 7 月.
[8] 米井 由美, 岩井原 瑞穂, 吉川 正俊, ``学習によるXML文書のコンテンツベースフィルタリング," 電子情報通信学会第 18 回データ工学ワークショップ第 5 回DBSJ年次大会(DEWS2007), 広島市, A7-3, 2007 年 3 月.

６．研究組織

(1)研究代表者

岩井原 瑞穂（IWAIHARA MIZUHO）
京都大学・情報学研究科・准教授
40253538

(2)研究分担者

吉川　正俊（YOSHIKAWA MASATOSHI）
京都大学・情報学研究科・教授
30182736

高田　英志（TAKADA HIDEYUKI）
立命館大学・情報理工学部・准教授
30378830

横田　裕介（YOKOTA YUSUKE）
立命館大学・情報理工学部・講師
70303881